UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,816	10/25/2001	Benjamin J. Parker	1688 (15723)	4720

33272 7590 03/02/2005

SPRINT COMMUNICATIONS COMPANY L.P.
6391 SPRINT PARKWAY
MAILSTOP: KSOPHT0101-22100
OVERLAND PARK, KS 66251-2100

EXAMINER	
ALOMARI, FIRAS B	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,816	PARKER ET AL.	
	Examiner	Art Unit	
	Firas Alomari	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 August 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/16/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. Claim 1 fails to point out what exactly is coupled to the pass-through router in line 15. claims 2-14 are rejected on virtue of their dependency on claim 1.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claim1-2, 4 and 5 are rejected under 35 U.S.C. 102(e) as being anticipated by Wadlow et al. (6,230,271).

AS per claim 1: Wadlow discloses a private network apparatus for connecting a user to an external Internet comprising:

- A plurality of security service pathways each providing a respective combination of security service features; (Col 3, lines 56-60; and Col 2, lines 40-46)
- A service selection dashboard allowing said user to select from a plurality of security service features for user traffic to and from said user; (Col 4; lines 32-34 and item MW in Figure 1 discloses a Maintenance Workstation used to inspect or change the behavior of devices)
- A network management server coupled to said service selection dashboard for storing a subscriber configuration in response to said user selected security service features; (Col 8, Lines 45-50)
- A pass-through router for coupling to said external internet; (Col 4, lines 36-38 and External router (ER) in FIG1)
- A service selection gateway coupled to said user for directing said user traffic to and from one of said service selection dashboard, said pass-through router, or one of said security service pathways; and (Col 4, lines 44-51 and Customer Local router (CLR) in FIG 1)

- A security service router for coupling said security service pathways to said external Internet; (Col 4, lines 36-38 and External router (ER) in FIG1)
- Wherein said service selection gateway directs said user traffic to said service selection dashboard if said subscriber configuration is in an initialized state; (Col 8, Lines 52-56)
- Wherein said service selection gateway directs said user traffic to a respective one of said security service pathways or to said pass-through router in response to said subscriber configuration after initialization by said service selection dashboard. (FIG 7 through FIG 17 show different communication pathways between a customer workstation and the public network in response to different security configuration by the customer)

As per claim 2: Wadlow discloses the apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall. (Col 6, Lines 59-64; a router with a filtering policy is a firewall)

As per claim 4: Wadlow discloses the apparatus of claim 1 wherein said security service pathways include at least one pathway having a content filter. (Col 8, Lines 12-26)

As per claim 5: Wadlow discloses the apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall and a content

filter. (Col 9, lines 59-64; shows a modification to a packet-filtering path to enable application and packet filtering)

3. Claims 14, 16-18 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Barrett (6,832,321).

As per claim 14: Barrett discloses a method of providing security service in a network interface to an external Internet, said method comprising the steps of:
Directing a user to a captive portal; (Col 8, lines 25-49)
Presenting security service features to said user; (Col 8; lines 25-49 and FIG. 6)
Storing a subscription profile for said user in response to security service features selected by said user through said captive portal; (Col 8, Lines 19-24 and Col 10, lines 23-29)
Receiving user traffic from said user destined for said external Internet at a service selection gateway; (Col 8, lines 59-66)
Determining from said subscription profile which security service features to apply to said user traffic; (Col 9, Lines 16-21)
If said subscription profile for said user includes any security service features, then re-directing said user traffic to a security service pathway corresponding to said security service features identified by said user profile; and
If said subscription profile for said user includes no security service features, then re- directing said user traffic to a pass-through router to said external internet. (Col 9 line 55 through Col 10 line 8)

As per claim 16: Barrett discloses the method of claim 15 wherein said firewall services comprise selectable grades of firewall protection including a high grade firewall protection, a medium grade firewall protection, and a low grade firewall protection. (FIG. 6 and Col 8 lines 25-50)

As per claim 17: Barrett discloses the method of claim 16 wherein said low-grade firewall protection comprises port blocking for outgoing user traffic. (Col 9, Lines 16-21/ the process could b modified to check the user-configurable security setting before establishing outbound connection)

As per claim 18: Barrett discloses the method of claim 16 wherein said medium grade firewall protection comprises port blocking for incoming and outgoing user traffic. (Col 9, Lines 16-21 and Col 8, Lines 27-35 / blocking outbound connection and inbound connections)

As per claim 19: Barrett discloses the method of claim 16 wherein said high-grade firewall protection comprises port blocking for outgoing user traffic and blocking of all incoming traffic not initiated by user. (Col 8, Lines 27-35 and Col 4, lines 1-7)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3, 6-7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wadlow et al. US (6,230,271) in view of Schneider et al. US (6,178,505).

As per claim 3: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show security service pathways with a virus scanner. However Schneider teaches the using of anti-virus system in a network apparatus to provide further protection to users data (Col 42, Lines 10-29). Therefore it would been obvious to ordinary skilled in the art at the time the invention was made to modify Wadlow system with the teaching of Schneider to include virus scanners on the security pathways. One would be motivated to do so in order to provide an additional level of security to the user by ensuring that the transmitted information came from authorized source and doesn't contain any viruses.

As per claim 6: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show security service pathways with a virus scanner. However Schneider teaches the using of anti-virus system in a network apparatus to provide further protection to users data (Col 42, Lines 10-29). Therefore it would been obvious to ordinary skilled in the art at the time the invention was made to modify Wadlow system with the teaching of Schneider to include virus scanners on the security pathways. One would be motivated to do so in order to provide an additional level of security to the user by ensuring that the transmitted information came from authorized source and doesn't contain any viruses.

As per claim 7: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show security service pathways with a virus scanner and a content filter. However Schneider teaches the using of anti-virus and (Col 42, Lines 10-29) and a content filter system (Col 40, Line 42 through Col 41, Line 29) in a network apparatus to provide protection to users data. Therefore it would been obvious to ordinary skilled in the art at the time the invention was made to modify Wadlow system with the teaching of Schneider to include virus scanners and a content filter on the security pathways. One would be motivated to do so in order to provide an additional level of security to the user by ensuring that the transmitted information came from authorized source doesn't contain any viruses and ensure that the user is authorized to view or use content of the data being transmitted.

As per claim 8: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show security service pathways with a virus scanner and a content filter. However Schneider teaches the using of anti-virus and (Col 42, Lines 10-29) and a content filter system (Col 40, Line 42 through Col 41, Line 29) in a network apparatus to provide protection to users data. Therefore it would been obvious to ordinary skilled in the art at the time the invention was made to modify Wadlow system with the teaching of Schneider to include virus scanners and a content filter on the security pathways. One would be motivated to do so in order to provide an additional level of security to the user by ensuring that the transmitted information came from authorized source doesn't contain any viruses and ensure that the user is authorized to view or use content of the data being transmitted.

6. Claims 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wadlow et al. US (6,230,271) in view of Barrett US (6,832,321)

As per claim 9: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show the firewalls providing different grades of firewall protection. However Barrett teaches the using of a firewall providing different grades of firewall protection (FIG. 6 and Col 8 lines 25-50). Therefore it would been obvious to ordinary skilled in the art at the time the invention was made to modify Wadlow

system with the teaching of Barrett to include a firewall providing different levels of protection. One would be motivated to do so in order to provide a security solution that doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21).

As per claim 10: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show the security pathways with firewalls providing high grade firewall protection, medium firewall protection and low firewall protection. However Barrett teaches the using of a firewall providing high firewall protection (Col 9, Lines 16-21 and Col 8, Lines 27-35 and Col 4, lines 1-7), medium firewall protection (Col 9, Lines 16-21 and Col 8, Lines 27-35) and low firewall protection (Col 9, Lines 16-21). Therefore it would been obvious to ordinary skilled in the art at the time the invention was made to modify Wadlow system with the teaching of Barrett to include a firewall providing high level protection, medium protection and low level protection. One would be motivated to do so in order to provide a security solution that enable the system to selectively grant access to the network from the client machine based on the user security preference (Col 4, Lines 54-57) and doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21).

As per claim 11: Wadlow discloses plurality of firewalls with different filtering polices but he doesn't explicitly show a low-grade firewall protection comprising

port blocking for outgoing traffic. However Barrett teaches the using of firewall providing low grade protection by blocking outgoing traffic (Col 9, Lines 16-21). Therefore it would been obvious to one ordinary skilled in the art at the time the invention was made to modify Wadlow system with teaching of Barrett to include a low grade firewall protection comprising of blocking of outgoing traffic. One would be motivated to do so in order to provide a security solution that enable the system to selectively grant access to the network from the client machine based on the user security preference (Col 4, Lines 54-57) and doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21).

As per claim 12: Wadlow discloses plurality of firewalls with different filtering polices but he doesn't explicitly show a medium grade firewall protection comprising port blocking for outgoing traffic and incoming. However Barrett teaches the using of firewall providing medium grade protection by blocking outgoing and incoming traffic (Col 9, Lines 16-21 and Col 8, Lines 27-35). Therefore it would been obvious to one ordinary skilled in the art at the time the invention was made to modify Wadlow system with teaching of Barrett to include a low grade firewall protection comprising of blocking of outgoing and incoming traffic. One would be motivated to do so in order to provide a security solution that enable the system to selectively grant access to the network from the client machine based on the user security preference (Col 4, Lines 54-57) and doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21).

As per claim 13: Wadlow discloses plurality of firewalls with different filtering polices but he doesn't explicitly show a high grade firewall protection comprising port blocking for outgoing traffic and incoming. However Barrett teaches the using of firewall providing medium grade protection by blocking outgoing and incoming traffic not initiated by user (Col 8, Lines 27-35 and Col 4, lines 1-7). Therefore it would been obvious to one ordinary skilled in the art at the time the invention was made to modify Wadlow system with teaching of Barrett to include a high grade firewall protection comprising of blocking of outgoing and incoming traffic not initiated by user. One would be motivated to do so in order to provide a security solution that enable the system to selectively grant access to the network from the client machine based on the user security preference (Col 4, Lines 54-57) and doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21).

7. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Barrett US (6,832,321) in view of Schneider et al. US (6,178,505)

As per claim 15: Barrett discloses a system providing security service features including firewalls but doesn't explicitly show a security service features including content filtering services, and a virus scanning service. However Schneider teaches the using of anti-virus and (Col 42, Lines 10-29) and a content filter system (Col 40, Line 42 through Col 41, Line 29) in a network apparatus to provide protection for users. Therefore it would been obvious to ordinary skilled

in the art at the time the invention was made to modify Barrett system with the teaching of Schneider to include virus scanners and a content filter on the security pathways. One would be motivated to do so in order to provide an additional level of security to the user by ensuring that the transmitted information came from authorized source and doesn't contain any viruses and to ensure that the user is authorized to view or use content of the data being transmitted.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 7:30 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

***

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100